AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0049] with the following amended paragraph:

[0049] The method 200 includes an act of altering standard connection establishment data to include address validation data (act 206). Act 206 can include the receiving computer system altering standard connection establishment data to include address validation data. For example, receiving messaging server ~~108~~ 109 can alter standard connection establishment data that would otherwise be sent to address 112 in response to receiving connection initiation data 111. When connection initiation data 111 indicates a TCP connection is to be established, receiving messaging server 109 can break the standard connection response data into a plurality of network packets. Alternately, when connection initiation data 111 indicates a TCP connection is to be established, receiving messaging server 109 can drop connection initiation data 111. In some embodiments, in response to receiving connection establishment data 111, receiving messaging server 109 alters standard connection establishment data to include a random string of characters (or other portion of non-standard data).

Please replace paragraph [0051] with the following amended paragraph:

[0051] In some embodiments, a messaging server that did not send connection initiation data receives altered connection establishment data. For example, when address 112 corresponds to messaging server 184, messaging server 184 can receive altered connection establishment data 118, which includes address validation data 114, from receiving messaging server 109. When received altered connection establishment data 118 was not received in response to corresponding connection initiation data, messaging server 184 may ~~simple~~ simply discard altered connection establishment data 118. Thus, when sending messaging server 107 is attempting to simulate (and thus hijack) a connection from messaging server 184, receiving messaging server 109 may not receive an appropriate response to address validation data 114. For example, receiving messaging server 109 may not receive an enhanced NOOP command echoing back a random sequence of characters contained in address validation data 114.

Please replace paragraph [0060] with the following amended paragraph:

[0060] Name server ~~108~~ 308 can store one or more records indicating authorized outgoing messaging servers for a domain. A record indicating authorized outgoing messaging servers for a domain. can be a DNS record, such as, for example, an RMX record , a TXT record, or a set of TXT records. A TXT record or a set of TXT records can contain text data or other data encoded in a textual form, such as, for example, XML instructions. Records indicating authorized outgoing messaging serves can be included in a DNS record set that indicates the electronic mail policy for a domain.

Please replace paragraph [0071] with the following amended paragraph:

[0071] It may be that messaging server 315 has been designated as an authorized computer system for sending electronic message from domain 305 but messaging server 316 has not been designated as an authorized computer system for sending electronic message from domain 305. Thus, authorized servers record 336 can be configured to contain a network address corresponding to messaging server 315 (and possibly network addresses for other computer systems) but not to contain a network address corresponding to messaging server 316. Accordingly, in response to receiving name server message 375, name server 308 can send name server response 377, which includes authorized servers list 378, to domain 307. Domain 307 can receive name server response ~~337~~ 377 and transfer name server response 377 to messaging server 317.

Please replace paragraph [0075] with the following amended paragraph:

[0075] The method 400 includes an act of providing the results of the determination to a message classification module (act 405). A message classification module can classify an electronic message as legitimate, unwanted, and/or unsolicited based on inputs provided to the message classification module. For example, messaging server 317 can provide the results of a determination with respect to messaging server computer system 316 (unauthorized) or with respect to messaging server 315 (authorized)~~)~~ to message classification module 328. Based on provided results indicating messaging server 316 is unauthorized (either alone or in combination with other provided inputs) electronic mail classification module 328 may classify electronic message 371 as unwanted and/or unsolicited.

Please replace paragraph [0098] with the following amended paragraph:

[0098] The method 600 includes an act of providing the relevant electronic message transmission policies to a message classification module (act 604). Act 604 can include a receiving computer system providing the relevant electronic message transmission policies to a message classification module. For example, messaging server 517 can provide relevant ETPs for domain 506 to message classification module 529. Based on relevant ETPs (either alone or in combination with other provided inputs), message classification module 529 may classify electronic message 575 as a legitimate electronic message or as an unwanted and/or unsolicited electronic message. Alternately, and when appropriate, messaging server 517 can provide relevant ETPs for domain ~~106~~ 506 to message classification module 553. Based on relevant ETPs (either alone or in combination with other provided inputs), message classification module 553 may classify electronic message 575 as a legitimate electronic message or as an unwanted and/or unsolicited electronic message.

Please replace paragraph [00106] with the following amended paragraph:

[00106] The method 700 includes an act of generating a puzzle input from one or more components of the electronic message (act 703). Act 703 can include a sending computer system generating a puzzle input from one or more components of the electronic message. For example, puzzle computation module 528 can generate a puzzle input ~~form~~ from one or more components (e.g., message body, message attachments, and message headers) of electronic message 545. Generating a puzzle input can include extracting, hashing, concatenating, or performing other operations on components of an electronic message.

Please replace paragraph [00125] with the following amended paragraph:

[00125] The method 700 includes an act of providing results of the determination to a message classification module (act 710). Act 710 can include a receiving computer system providing results of the determination to a message classification module. For example, messaging server 517 can provide results of a determination with respect to messaging server 516 to (indicating that messaging server 516 did or did not expend~~ed~~ processor cycles) to message classification module 529. Based on a provided determination indicating that messaging server 516 did expended computational resources (either alone or in combination with other provided inputs), message classification module 529 may classify electronic message 545 as legitimate. On the other hand, based on a provided determination indicating that messaging server 516 potentially did not expend computational resources (either alone or in combination with other provided inputs), message classification module 529 may classify electronic message 545 as unwanted and/or unsolicited. Alternately and when appropriate, messaging server 517 can provide results indicating that messaging server 516 did or potentially did not expended computational resources to message classification module 553.

Please replace paragraph [00138] with the following amended paragraph:

[00138] Accordingly, electronic message senders and ~~receives~~ receivers may agree to mutually configured mechanisms for reducing unwanted and unsolicited electronic messages. Thus, it may be that combinations of results from different configured mechanisms are provided to a message classification module. For example, an electronic message recipient may both check for adherence to an ETP and check for proof of effort by the electronic message sender and provide the results of both checks to a message classification module. Proof of effort can include providing a hash collision, a solution to a cryptographic problem, a solution to a memory bound problem, a solution to a reverse Turing test. A receiving domain can check for provided proof of effort and provide the results of the check to a message classification module.

Please replace paragraph [00139] with the following amended paragraph:

[00139] In this description and in the following claims, a "schema" is defined as an expression of a shared vocabulary between a plurality of computer systems that allows the plurality of computer systems to process documents according to the expressed shared vocabulary. For example, an eXtensible Markup Language ("XML") schema can define and describe a class of XML documents using schema constructs of an XML schema language. These schema constructs can be used to constrain and document the meaning, usage, and relationships of data types, elements and their content, attributes and their values, entities and their contents, and notations, as used in XML documents. Thus, any computer system that can access an XML schema can process XML documents in accordance with the XML schema. Further, any computer system that can access an XML schema can compose or modify XML documents for use by other computer systems that can also access the XML schema.

Please replace paragraph [00149] with the following amended paragraph:

[00149] Likewise, computer system 820 includes input/output interface 846, through which computer system 820 receives data from external sources and/or transmits data to external sources. Input/output interface 846 is coupled to modem ~~554~~ 854 (e.g., a standard modem, a cable modem, or digital subscriber line ("DSL") modem) via data link 859, through which computer system 820 receives data from and/or transmits data to external sources. As depicted in Figure 8, input/output interface 846 and modem 854 facilitate the exchange of data with remote computer system 893 via link 852. Link 852 represents a portion of a network and remote computer system 893 represents a node of the network. For example, remote computer system 893 may be a sending computer system that sends an electronic message to computer system 820. On the other hand, remote computer system 893 may be a receiving computer system that receives an electronic mail message from computer system 820.